

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-069175

(43)Date of publication of application : 16.03.2001

(51)Int.Cl.

H04L 12/66

G06F 13/00

H04L 12/56

(21)Application number : 11-242013

(71)Applicant : NTT DOCOMO INC

(22)Date of filing : 27.08.1999

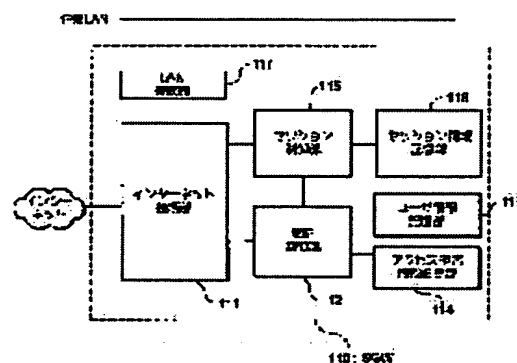
(72)Inventor : TAKAHASHI TATSUO  
TAKESHITA ATSUSHI  
SEKIGUCHI KATSUMI

## (54) METHOD AND DEVICE FOR SESSION INFORMATION MANAGEMENT

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To prevent resources for session information from being used up at a low cost while securing a stable communication by providing a session information deletion stage, etc., which deletes session information corresponding to state confirmation when an answer showing that a connection state is normal is not obtained.

**SOLUTION:** When there is no answer to a state confirmation message, a session control part 115 decides that a mobile terminal to which an IP address whose state has been confirmed is assigned is disconnected from a packet gateway and the old session corresponding to the IP address is dead. Then the session control part 115 selects a candidate session to be deleted from session information stored in a session information storage part 116. A 'dead session' is possibly included in the stored session information and deleted to eliminate the exhaustion of session resources.



## LEGAL STATUS

[Date of request for examination]

02.07.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the  
examiner's decision of rejection or application  
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of  
rejection][Date of requesting appeal against examiner's decision  
of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)

RECEIVED JANUARY 1971

1971 JAN 19 10 10 AM

(11)特許出願公開番号  
特開2001-69175  
(P2001-69175A)

(43)公開日 平成13年3月16日(2001.3.16)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	デモコード <sup>7</sup> (参考)
H 0 4 L 12/66		H 0 4 L 11/20	B 5 B 0 8 9
G 0 6 F 13/00	3 5 3	G 0 6 F 13/00	3 5 3 C 5 K 0 3 0
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 Z

審査請求 未請求 請求項の数11 O.L (全 15 頁)

(21)出願番号 特願平11-242013

(22)出願日 平成11年8月27日(1999.8.27)

(71)出願人 392026693

株式会社エヌ・ティ・ティ・ドコモ  
東京都千代田区永田町二丁目11番1号

(72)発明者 高橋 竜男

東京都港区虎ノ門二丁目10番1号 エヌ・  
ティ・ティ移動通信網株式会社内

(72)發明者 竹下 敦

東京都港区虎ノ門二丁目10番1号 エヌ・  
ティ・ティ移動通信網株式会社内

(74) 代理人 100098084

弁理士 川▲崎▼ 研二 (外2名)

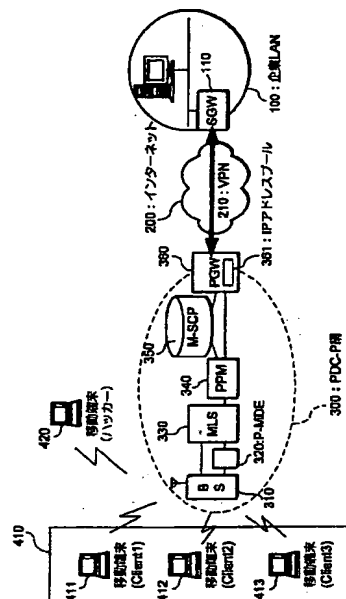
**最終頁に続く**

(54)【発明の名称】 セッション情報管理方法およびセッション情報管理装置

(57) 【要約】、*「『新編』の成立と展開」*

【課題】 クライアントとサーバとを接続する仮想私設網において、安定的な通信を確保しながら低コストでセッション情報の資源枯渇を防止する。

【解決手段】 セキュリティゲートウェイ110は、総セッション数制限の範囲をこえた時点で「死んでいる」可能性の高い削除候補セッションを選択し、順次セッションが生きているか否かの状況確認を行い、「死んでいる」セッションと確認できたセッションを削除していくので、削除ミスの可能性を極めて小さくすることができる。また、キープアライブパケットを使用しなくても「死んでいる」セッションを削除できるので、キープアライブパケットに対する課金がなくなり、移動端末400のユーザは通信コストを削減することができる。



**BEST AVAILABLE COPY**

## 【特許請求の範囲】

【請求項1】 クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶段階と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において設定可能な総セッション数をこえた場合には、記憶されている前記セッション情報から削除すべき候補を所定の規則に従って選択する削除候補選択段階と、

前記選択された削除候補のセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除段階とを備えることを特徴とするセッション情報管理方法。

【請求項2】 請求項1に記載のセッション情報管理方法において、

前記所定の規則に従って選択される優先順位は、生成されてからの経過時間が長い前記セッション情報である程高いことを特徴とするセッション情報管理方法。

【請求項3】 請求項1に記載のセッション情報管理方法において、

前記所定の規則に従って選択される優先順位は、最後に使用されてからの経過時間が長い前記セッション情報である程高いことを特徴とするセッション情報管理方法。

【請求項4】 請求項1に記載のセッション情報管理方法において、

クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、当該状況確認に対応する前記セッション情報について、前記所定の規則に従って選択される優先順位を低く設定する優先順位設定段階を備えることを特徴とするセッション情報管理方法。

【請求項5】 クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶段階と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択段階と、

前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、

前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除段階とを備えることを特徴とするセッション情報管理方法。

【請求項6】 クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、

クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶段階と、

前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択段階と、

前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、

クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、前記前記セッション設定要求を拒絶する拒絶段階とを備えることを特徴とするセッション情報管理方法。

【請求項7】 請求項6に記載のセッション情報管理方法において、

前記セッション設定要求を拒絶する場合には、当該セッション設定要求に含まれる前記認証情報およびアドレス情報をアクセス拒否情報として記憶する拒否情報記憶段階を備えることを特徴とするセッション情報管理方法。

【請求項8】 請求項7に記載のセッション情報管理方法において、

前記セッション設定要求が前記アクセス拒否情報として記憶された認証情報およびアドレス情報と一致する場合には前記前記セッション設定要求を拒絶する第2の拒絶段階を備えることを特徴とするセッション情報管理方法。

【請求項9】 クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、

クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、クライアントの認証情報およびアドレス情報とを対応つけてセッション情報として記憶するセッション情報記憶手段と、

前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において設定可能な総セッション数をこえた場合には、記憶されている前記セッション

ン情報から削除すべき候補を所定の規則に従って選択する削除候補選択手段と、  
前記選択された削除候補のセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、  
前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除手段とを備えることを特徴とするセッション情報管理装置。

【請求項10】 クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、  
クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶手段と、  
前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択手段と、  
前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、  
前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除手段とを備えることを特徴とするセッション情報管理装置。

【請求項11】 クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、  
クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶手段と、  
前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択手段と、  
前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、  
クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、前記前記セッション設定要求を拒絶する拒絶手段とを備えることを特徴とするセッション情報管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、クライアントと

サーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理方法およびセッション情報管理装置に関する。

【0002】

【従来の技術】従来より、通信端末装置（クライアント）が電話網を介して最寄りのインターネット接続点に接続（いわゆるダイヤルアップ接続）し、さらに、インターネットを介してサーバ側のネットワーク（例えば企業LAN（Local Area Network））に接続する場合において、インターネット上を安全に通過するために仮想私設網（Virtual Private Network：VPN）を構築するいわゆるダイヤルアップVPNが知られている。仮想私設網とは、暗号技術や、認証技術、トンネリング技術などを利用して、インターネット上においても専用線と同様の安全性および利便性を有する通信を実現する技術である。このような仮想私設網機能を実現するネットワークコンポーネントをセキュリティゲートウェイ（Security Gateway：SGW）という。

【0003】仮想私設網においては、通常はIP（Internet Protocol）アドレスを用いて通信相手を識別する。ところで、IPアドレスは、クライアント毎に固定されている場合もあるが、クライアントがダイヤルアップ接続を行っている場合には、接続を行う度に異なっている場合がある。具体的には、ダイヤルアップクライアントに割り当てるためのIPアドレスを一定数確保しているインターネット接続点に電話網を介して接続要求を行うことによって、ダイヤルアップクライアントは利用可能なIPアドレスが適宜割り当てられるようになっていく。従って、ダイヤルアップVPNにおいては、仮想私設網を終端するクライアントがダイヤルアップ接続を行っている場合には、仮想私設網の他端となるセキュリティゲートウェイはIPアドレスからクライアントを識別することができないことになる。

【0004】そこで、セキュリティゲートウェイはIPよりも上位層のプロトコルでクライアントの認証を行う必要があり、一般的にはユーザIDおよびパスワードを組み合わせた情報や、デジタル署名などの情報を用いて認証を行っている。このような認証を行った後、クライアントおよびセキュリティゲートウェイ間の通信を行うために、IPアドレス等の情報や仮想私設網におけるセキュリティポリシーなどのネゴシエーションを行う。クライアントおよびセキュリティゲートウェイは、ネゴシエーションにおける情報を双方でセッション情報として保存する。このようにしてクライアントがセキュリティゲートウェイに接続することによって、企業LAN内にいるのと同様の環境で、企業内各種サーバに接続し、所望のサービスを利用することが可能となっている。

【0005】

【発明が解決しようとする課題】このような仮想私設網のセッション設定から解放までは、

- (1) クライアントからインターネット接続点へ接続
- (2) クライアント・セキュリティゲートウェイ間にセッション設定
- (3) クライアント・サーバ間通信
- (4) クライアント・サーバ間セッション断
- (6) クライアント・セキュリティゲートウェイ間セッション断
- (7) クライアントからインターネット接続点へのコネクション断

という手順が踏まれるのが通常である。しかしながら、クライアント・インターネット接続点間の接続が切断されてしまい、クライアントが正常な手順を踏まない状態で終了してしまう場合も生じることがある。例えば、クライアントの電源が遮断されてしまった場合や、インターネット接続点の故障、無線網を介してインターネット接続点に接続しているクライアントが圏外に移動してしまった場合などが考えられる。なお、以下の説明において、クライアント・インターネット接続点間が接続されている状態を「生きているセッション」といい、クライアント・インターネット接続点間の接続が切断されている状態を「死んだセッション」というものとする。

【0006】このように、正常な手順を踏まずに終了すると、セッションに関して以下のような問題が生じる。クライアントは電話網を介してインターネットに接続しているため、クライアント・インターネット接続点間の接続状態（セッションの生死）を直ちに検出することができず、これに対してセキュリティゲートウェイはインターネットに接続しているためクライアント・インターネット接続点間の接続状態を直接検出することはできない。サーバからクライアントへパケットを送信するシーケンスの途中でクライアント・インターネット接続点間の接続が切断された場合は、パケットはクライアントへ到達しないので、セキュリティゲートウェイはクライアント・インターネット接続点間の接続が切断された状態をパケットの不達によって間接的に検出する。

【0007】しかしながら、パケットの不達を検出できないような場合、例えば、サーバがクライアントから要求待ちであるような場合や、クライアント・サーバ間のセッションが確立していないような場合、あるいは、セッションが確立していても使用されていない場合には、セキュリティゲートウェイはクライアント・インターネット接続点間の接続が切断された状態を直接的にも間接的にも検出することができない。このようにセキュリティゲートウェイがクライアント・インターネット接続点間の接続を検出できないために、「死んだセッション」をセキュリティゲートウェイが保存したままになると、セキュリティゲートウェイではセッション資源が枯渇してしまうという問題が生じる。あるいは、電話網側の回線状況などが原因で、インターネット接続点への接続が切断されたクライアントが再度インターネット接続点に

接続した場合は、以前に使用していたものとは異なるIPアドレスが割り当てられるので、クライアントがセキュリティゲートウェイに仮想私設網セッション設定を再要求した場合には、以前のセッション情報が保存されているために新しいセッションの設定を拒絶してしまうという問題も生じる。セキュリティゲートウェイでは、同一ユーザIDのクライアントが同時に複数のセッションを設定することはセキュリティ上の理由で制限しているからである。このような問題を解決するためには、一定時間利用されないセッションをセキュリティゲートウェイが自動的に削除するように設定することも可能であるが、このような場合はクライアント側が長時間通信を行わない場合にはセッションを削除されてしまうという不都合があり、クライアントには不便になっていく。

【0008】そこで、従来は一定周期毎にサーバからクライアントに状態確認のパケット（キープアライブパケット）を送り、クライアントはキープアライブパケットを受け取るとただちに正常である旨の応答を行うようにして、サーバは規定時間以内に応答が帰ってこなかった場合にクライアントがセッションを停止したと判断してセッション情報を削除する、という対応がなされていた。しかしながら、クライアントが接続している電話網が、送受信データ量に対して課金される、いわゆるパケット交換方式の電話網である場合、このようなキープアライブパケットを用いると、一定周期毎にパケットの交換が行われ、個々のキープアライブパケットに対して課金が行われてしまうので、クライアント側ユーザの通信コストがかさんでしまうという問題があった。あるいは、電話網やインターネットの一時的な輻輳などによりパケットの伝達遅延が生じてしまった場合には、キープアライブパケットに対する応答が規定時間内に戻らないので、セッションは生きているにもかかわらずセッション情報が削除されてしまい、安定した通信を行うことができないという問題もあった。このように、従来のセッション管理方法においては、安定的な通信を確保しながら低コストでセッション情報の資源枯渇を防止することは困難であった。

【0009】本発明は、上述した課題を解決するためになされたものであり、安定的な通信を確保しながら低コストでセッション情報の資源枯渇を防止することができるセッション情報管理方法およびセッション情報管理装置を提供することを目的としている。

【0010】

【課題を解決するための手段】上述した課題を解決するために、請求項1に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセ

セッション情報を生成して記憶するセッション情報記憶段階と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において設定可能な総セッション数をこえた場合には、記憶されている前記セッション情報から削除すべき候補を所定の規則に従って選択する削除候補選択段階と、前記選択された削除候補のセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除段階とを備えることを特徴とする。

【0011】請求項2に記載の発明は、請求項1に記載のセッション情報管理方法において、前記所定の規則に従って選択される優先順位は、生成されてからの経過時間が長い前記セッション情報である程高いことを特徴とする。請求項3に記載の発明は、請求項1に記載のセッション情報管理方法において、前記所定の規則に従って選択される優先順位は、最後に使用されてからの経過時間が長い前記セッション情報である程高いことを特徴とする。請求項4に記載の発明は、請求項1に記載のセッション情報管理方法において、クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、当該状況確認に対応する前記セッション情報について、前記所定の規則に従って選択される優先順位を低く設定する優先順位設定段階を備えることを特徴とする。

【0012】請求項5に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶段階と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択段階と、前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除段階とを備えることを特徴とする。

【0013】請求項6に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、クライアントの認証情報およびアド

レス情報を含んだセッション設定要求をうけるセッション設定要求段階と、前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶段階と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択段階と、前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、前記前記セッション設定要求を拒絶する拒絶段階とを備えることを特徴とする。請求項7に記載の発明は、請求項6に記載のセッション情報管理方法において、前記セッション設定要求を拒絶する場合には、当該セッション設定要求に含まれる前記認証情報およびアドレス情報をアクセス拒否情報として記憶する拒否情報記憶段階を備えることを特徴とする。請求項8に記載の発明は、請求項7に記載のセッション情報管理方法において、前記セッション設定要求が前記アクセス拒否情報として記憶された認証情報およびアドレス情報と一致する場合には前記前記セッション設定要求を拒絶する第2の拒絶段階を備えることを特徴とする。

【0014】請求項9に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、クライアントの認証情報およびアドレス情報とを対応つけてセッション情報として記憶するセッション情報記憶手段と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において設定可能な総セッション数をこえた場合には、記憶されている前記セッション情報から削除すべき候補を所定の規則に従って選択する削除候補選択手段と、前記選択された削除候補のセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除手段とを備えることを特徴とする。

【0015】請求項10に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶

するセッション情報記憶手段と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択手段と、前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除手段とを備えることを特徴とする。

【0016】請求項11に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶手段と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択手段と、前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、前記前記セッション設定要求を拒絶する拒絶手段とを備えることを特徴とする。

【0017】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態について説明する。

【0018】[1. 実施形態の構成]

[1-1. 全体構成] 図1は実施形態の全体構成を示す図である。図1に示すように、本実施形態では、企業LAN100に対して、セキュリティゲートウェイ110を端末としてインターネット200に設定された仮想私設網210および移動通信網300を介して移動端末411、412、413、420（特定を要さない場合は移動端末400と記す）が接続できるようにしている。

【0019】本実施形態では、移動通信網300にはPDC移動パケット通信システム（Personal Digital Cellular - Packet: PDC-P）を用いており、移動通信網300は、基地局（Base Station: BS）310、パケット用基地局変復調装置（Packet Modulation/Demodulation Equipment: P-MDE）320、加入者交換機（Mobile Local Switch: MLS）330、パケット加入者系処理装置（Packet Processing Module: PPM）

340、移動通信サービス制御装置（Mobile Service Control - Point: M-SCP）350、パケットゲートウェイ（Packet GateWay: PGW）360を備えて構成されている。基地局310は、パケット通信機能を有するパケット用基地局変復調装置320に接続されており、移動端末400への高速なパケットエアーフェイスを提供する。パケット加入者系処理装置340は、基地局310を介して移動端末400と対向し、パケットを送受信するものであり、無線区間のパケットの組立・分解、認証、秘匿、課金などを行う。本実施形態では、企業LAN100から移動端末400への下りパケットに対する課金ポイントとして機能し、移動端末400から下りパケットに対する応答を示すACK（Acknowledge）を受信した時点で課金を行う。移動通信サービス制御装置350は、移動端末400の存在するエリアや加入者のサービス情報を記憶する網内データベースを備え、パケットゲートウェイ360は、インターネット200など他網から移動端末400へのパケット着信時に移動通信サービス制御装置350が有する位置情報へアクセスして、移動端末400の存在するエリアを管理しているパケット加入者系処理装置340へルーティングする。

【0020】パケットゲートウェイ360は、インターネット接続点としての機能とともに、移動端末400から企業LAN100への上りパケットへの課金ポイントとしての機能を有している。パケットゲートウェイ360は、IPアドレスプール361を備えており、移動端末400から接続要求があった時点で利用可能なIPアドレスの中から任意の一つを選択的に割り当てる。移動端末400は、仮想私設網210を介して企業LAN100へ接続する場合にはインターネット接続点であるパケットゲートウェイ360へ接続を行い、接続を行う度に異なるIPアドレスの割り当てを受けることによって、企業LAN100へパケットを送信することができるようになる。パケットゲートウェイ360は、インターフェイス200にパケットが送信された時点で課金を行う。

【0021】本実施形態においては、移動端末411、412、413（特定を要さない場合は移動端末410と記す）は、企業LAN100に対する正当な権限を有するユーザが使用する通信端末装置であり、移動端末420は、企業LAN100に対して正当なアクセス権限を有さない者（いわゆるハッカー）が使用する通信端末装置である。正当権限を有する移動端末410それぞれのユーザには企業LAN100における固有のユーザIDが割り当てられている。本実施形態では、移動端末411のユーザには“Client1”というユーザIDが割り当てられ、移動端末412のユーザには“Client2”というユーザIDが割り当てられ、移動端末413のユーザには“Client3”というユーザIDが割り当てられて



おり、これらのユーザIDは、後に詳しく説明するように、企業LAN100内において各移動端末410のユーザを識別する情報として管理されている。なお、移動端末420のユーザであるハッカーにはユーザIDは割り当てられておらず、正当権限者からユーザIDおよびパスワードなどの認証情報を不正に入手して企業LAN100に対して接続を試みる。本実施形態では、ユーザID、パスワード、IPアドレスなどの情報を用いて、企業LAN100と移動端末400とのセッションが設定されると、後に詳しく説明するようにセキュリティゲートウェイ110および移動端末400はセッション情報をそれぞれ保存して、仮想私設網210上における通信を安定的に行うとともに第三者の不正なアクセスを防止するようになっている。

【0022】[1-2. セキュリティゲートウェイの構成] 次に、セキュリティゲートウェイ110についてより詳細に説明する。図2は、セキュリティゲートウェイ110の機能構成を示すブロック図である。セキュリティゲートウェイ110は、インターネット200とインターフェイスであるインターネット接続部111、認証を制御する認証制御部112、ユーザIDやパスワードなどのユーザ認証情報を記憶するユーザ情報記憶部113、不正なアクセスを拒否するための情報を記憶するアクセス拒否情報記憶部114、セッションに関する各種制御を行うセッション制御部115、セッション情報を記憶するセッション記憶部116、および、企業LAN100内のインターフェイスであるLAN接続部117を備えている。

【0023】ここで、図3を参照しながら、セッション情報116、ユーザ情報記憶部113、およびアクセス拒否情報記憶部114に記憶される情報について説明しておく。セッション情報記憶部116には、それぞれ異なるセッション番号毎にクライアントのIPアドレスおよびユーザIDを対応付けたセッション情報が記憶されている。セッション番号が付される規則については、後に説明する。ユーザ情報記憶部113には、企業LAN100へのアクセス権限を有する各ユーザに割り当てられたユーザID毎に各ユーザが設定したパスワードを対応付けたユーザ情報が記憶されている。また、アクセス拒否情報記憶部114には、不正なアクセスと判定されたユーザID毎に、不正なアクセスを行った際に用いられたIPアドレスが対応づけられたアクセス拒否情報が記憶されている。アクセス拒否情報が示すユーザIDは、ハッカーが正当なユーザから不正に入手したユーザIDであって、ユーザID自体はユーザ情報記憶部113に記憶された正当な情報である。本実施形態ではユーザIDやパスワードを不正に入手した場合であっても、IPアドレスを用いて正当なセッション設定要求であるか否かを判定できるようになっている。

【0024】[2. 実施形態の動作] 次に、本実施形態

の動作として、図4～図6に示すフローチャートを参照しながらセキュリティゲートウェイの動作を説明した後に、図7～図9に示すシーケンスを参照しながら全体の具体的な動作を説明する。

【0025】[2-1. セキュリティゲートウェイの動作]

[2-1-1. セッション設定要求時の動作] 図4は、セキュリティゲートウェイ110のセッション設定要求時における動作を示すフローチャートである。セキュリティゲートウェイ110は、セッション設定要求を受けると(S1)、まず当該セッション要求についての認証を行う(S2)。ここでは、認証制御部112は、先に説明したユーザ情報記憶部113およびアクセス拒否情報記憶部114に記憶された情報(図3参照)に基づいては正当なユーザからの要求か否かを判定する。ステップS2の認証において、正当なユーザからのセッション設定要求ではないと判定した場合は(S2; NG)、ステップS1において受けたセッション設定要求を拒絶する(S3)。

【0026】一方、ステップS2の認証において、正当なユーザからのセッション設定要求であると判定した場合は(S2; OK)、次に、同時接続セッション数のチェックを行う(S4)。同時接続セッション数のチェックとは、同一のユーザIDを有するクライアントが同時にセッション設定を行うことを制限するための処理である。具体的には、セッション要求を行ったクライアントが示すユーザIDと同一のユーザIDに対応したセッション情報が当該チェック時においてセッション情報記憶部116に記憶されている場合には、同時接続セッション数をこえていると判定する。ステップS4において、同時接続セッション数をこえていないと判定した場合は(S4; OK)、当該セッション設定要求に対するセッション設定処理を行う(S5)。セッション設定処理は、サーバ側セキュリティゲートウェイ110のセッション資源の枯渇を解消するための処理であり、より詳しくは、図5および図7を参照しながら後に説明する。一方、ステップS4において、同時接続セッション数をこえていると判定した場合は(S4; NG)、不正接続防止処理を行う(S6)。不正接続防止処理は、すでにセッション情報が記憶されているユーザIDと同一のユーザIDを示すセッション設定要求が、正当なユーザからのものであるか否かを判定する処理であり、より詳しくは、図6～図9を参照しながら後に説明する。

【0027】[2-1-2. セッション設定処理] 次に、図5に示すフローチャートを参照しながら、セッション設定処理(図4: S5)について説明する。セッション設定処理では、セキュリティゲートウェイ110はまず総セッション数制限チェックを行う(S51)。セッション情報記憶部116に記憶することが可能な総セッション数には予め制限が設けられており、この制限を

こえてセッション設定要求があった場合にはサーバ側のセッション資源が枯渇する。そこで、セッション制御部115は、セッション設定要求時においてセッション情報記憶部116に記憶されているセッション数が当該制限の範囲内であるか否かを判定する。

【0028】ステップS51のチェックにおいて、セッション数が当該制限の範囲内であると判定した場合は（S51；OK）、セッション制御部115は、セッション設定要求に対するセッション設定を行う（S52）。一方、ステップS51のチェックにおいて、セッション数が当該制限の範囲内ではないと判定した場合は（S51；NG）、セッション制御部115は、セッション情報記憶部116に記憶されているセッション情報の中から、削除すべき候補セッションを選択する（S53）。記憶されているセッション情報の中には、上述したような「死んでいるセッション」が含まれている可能性があり、このような「死んでいるセッション」を削除することによってセッション資源の枯渇を解消することができる。

【0029】本実施形態では、次に説明する2種類のアルゴリズムのいずれかを用いて、削除してよい可能性の高いセッションを選択する。

#### ①FIFO (First In First Out)

最も古く作成されたセッションを削除するアルゴリズムである。このアルゴリズムを用いて削除セッションの候補を選択する場合には、例えば、セッション制御部115は、セッションを作成した順番にセッション番号が付されるようにセッション情報を生成し、セッション情報記憶部116に記憶されているセッション情報の中から最も小さなセッション番号を有するものを、削除セッション候補として選択する。このような場合は、新規にセッション情報を生成する際に、その時点で最も大きなセッション番号が付されるようにすればよい。

#### ②LRU (Last Recently Used)

最も古く使用されたセッションを削除するアルゴリズムである。このアルゴリズムを用いて削除セッションの候補を選択する場合には、例えば、セッション制御部115は、セッションを使用した順番にセッション番号が付されるようにセッション情報を生成し、セッション情報記憶部116に記憶されているセッション情報の中から最も小さなセッション番号を有するものを、削除セッション候補として選択する。この場合は、通信が行われる毎にその時点で最も大きなセッション番号が再度付されるようにすればよい。

【0030】ステップS53において削除候補セッションの選択を行うと、セッション制御部115は、選択された削除候補セッションに対応するクライアントに対して状況確認メッセージを送信し（S54）、当該クライアントから正常な応答があったか否かを判定する（S55）。ここでは、所定期間内にクライアントから応答が

ない場合や、予め規定された応答とは異なる応答あるいは何らかの異常を示す応答（異常応答）があった場合に、クライアントからの応答がないと判定される。ステップS55の判定において、クライアントからの応答があったと判定した場合は（S55；あり）、ステップS53において選択されたセッションを削除候補の最後に置き換え（S56）、ステップS53に移行して再度削除候補セッション選択を行う。例えば、最も小さなセッション番号の付されたセッション情報を削除候補として選択している場合であれば、当該セッション情報中のセッション番号をその時点で最も大きなセッション番号に更新することによって、削除候補の最後に置き換える。一方、ステップS55の判定において、クライアントからの応答がなかったと判定した場合は（S55；なし）、ステップS53において選択した当該セッションを削除して、セッション要求に対するセッションを設定する（S57）。

【0031】[2-1-3. 不正接続防止処理] 次に、図6に示すフローチャートを参照しながら、不正接続防止処理（図4：S6）について説明する。不正接続防止処理では、セキュリティゲートウェイ110は旧セッションのIPアドレスに対して状況確認メッセージを送信し（S61）、当該状況確認メッセージに対する応答が有るか否かを判定する（S62）。セッション制御部115は、セッション情報記憶部116に記憶されているセッション情報から、セッション設定要求を行っているクライアントのユーザIDと同一のユーザIDに対応して記憶されているIPアドレスを旧セッションのIPアドレスとして抽出し、当該IPアドレスを宛先とした状況確認メッセージパケットを送信する。なお、状況確認メッセージには、同一のユーザIDを示すセッション設定要求があった旨を警告するメッセージが含まれている。

【0032】ステップS62の判定において、状況確認メッセージに対する応答がなかった場合は（S62；なし）、セッション制御部115は、状況確認を行ったIPアドレスが割り当てられた移動端末400とパケットゲートウェイ360（インターネット接続点）との接続が切断され、当該IPアドレスに対応した旧セッションが死んでしまったと判定し、旧セッションを削除してセッション設定要求に対して新セッションを設定する（S63）。より具体的には、状況確認を行ったIPアドレスに対応したセッションが死んでいる場合に、同一ユーザIDを示す新たなセッション要求がある場合とは、何らかの理由で移動端末400とパケットゲートウェイ360との接続が切断された後に、再度接続し直したために通信端末400に対して新たなIPアドレスが割り当てられた可能性が高い。そこで、セッション制御部115は、このような場合にはセッション接続要求は正当なユーザからのものであると判定する。また、同時セッ

セッション数制限を解消するために旧セッションをセッション情報記憶部から削除する。これに対して、ステップS62の判定において、状況確認メッセージに対する応答があった場合は(S62;あり)、状況確認を行ったIPアドレスに対応したセッションは生きている、すなわち、当該IPアドレスの割り当てられた移動端末400と企業LAN100は接続された状態にあるにもかかわらず、第三者が不正に接続しようとしていると判定し、セッション設定を拒絶する(S64)。

#### 【0033】[2-2. 実施形態の具体的動作]

[2-2-1. 総セッション数制限をこえた場合] まず、図7を参照しながら、総セッション数制限が2であるセキュリティゲートウェイ110に対して、3以上の移動端末400がそれぞれセッション設定要求を行うことによって、総セッション数制限の範囲をこえた場合の動作について説明する。図7においては、図1に示す移動端末411がユーザID“Client1”として、移動端末412がユーザID“Client2”として、移動端末413がユーザID“Client3”として、それぞれセッション設定要求を行う。なお、図7においては、各移動端末400に対して割り当てられたIPアドレスに関する情報は省略している。

【0034】移動端末411がユーザID“Client1”としてセキュリティゲートウェイ110へのセッション設定要求を行う(S101)。このとき、セッション制御部115は、セッション情報記憶部116に記憶されているセッション情報を参照して総セッション数制限の範囲内であると判定し、新たにセッション情報を生成する。この新たなセッション情報には、この時点で最も大きなセッション番号#1が付される。新たなセッション情報を生成するとセキュリティゲートウェイ110は、移動端末411に対してセッション設定の応答を行い(S102)、移動端末411と企業LAN100との仮想私設網210を介した通信を行うことができるようになる。

【0035】次に、移動端末412がユーザID“Client2”としてセキュリティゲートウェイ110へのセッション設定要求を行う(S103)。このとき、セッション制御部115は、セッション情報記憶部116に記憶されているセッション情報を参照して総セッション数制限の範囲内であると判定し、新たにセッション情報を生成する。この新たなセッション情報には、この時点で最も大きなセッション番号#2が付される。新たなセッション情報を生成するとセキュリティゲートウェイ110は、移動端末412に対してセッション設定の応答を行い(S104)、移動端末412と企業LAN100との仮想私設網210を介した通信を行うことができるようになる。

【0036】セキュリティゲートウェイ110における総セッション数制限は2であるから、この時点でセッシ

ョン資源が枯渇しており、その後に移動端末413がユーザID“Client3”としてセキュリティゲートウェイ110へのセッション設定要求を行うと(S105)、セッション制御部115は、セッション情報記憶部116に記憶されているセッション情報を参照して総セッション数制限の範囲をこえたと判定する。そこで、セッション制御部115は、この時点で最も小さなセッション番号#1の付されたセッション情報を「死んでいる」可能性の高い削除候補セッションとして選択し、セッション番号#1に対応して記憶されているユーザID“Client1”を示す移動端末411に対して状況確認メッセージを送信する(S106)。移動端末411が状況確認メッセージに対して正常な応答を行うと(S107)、セッション制御部115は、選択されたセッション情報のセッション番号#1をこの時点で最も大きなセッション番号#3に更新する。セッション番号#1がセッション番号#3に更新されることによって、“Client1”に対応するセッション情報は削除候補の最後に置き換えられ、この時点で最も小さなセッション番号は#2となる。

【0037】ところで、移動端末412は、セッション設定後に圏外へ移動しており(S108)、パケットゲートウェイ360との接続が切断されている。従って、セッション番号#2の付されたセッションは「死んだ」状態になっている。しかしながら、セキュリティゲートウェイ110においては、移動端末412とパケットゲートウェイ360との接続が切断されていることは検出していないので、セッション制御部115はセッション番号#2の付されたセッション情報を削除候補として選択し、セッション番号#2に対応して記憶されているユーザID“Client2”を示す移動端末412に対して状況確認メッセージを送信する(S109)。移動端末412とパケットゲートウェイ360との接続が切断されているので、この状況確認メッセージは移動端末412に到達せず、セキュリティゲートウェイ110に対しては何ら応答がなされない、あるいは異常な応答がなされることになる(S110)。セッション制御部115はセッション番号#2の付されたセッションは「死んでいる」と判定してセッション情報を削除し、移動端末413がユーザID“Client3”として行ったセッション設定要求に対するセッション情報を生成する。この新たなセッション情報には、この時点で最も大きなセッション番号#4が付される。新たなセッション情報を生成するとセキュリティゲートウェイ110は、移動端末413に対してセッション設定の応答を行い(S111)、移動端末413と企業LAN100との仮想私設網210を介した通信を行うことができるようになる。

【0038】このように、セキュリティゲートウェイ110は、総セッション数制限の範囲をこえた時点で「死んでいる」可能性の高い削除候補セッションを選択し、順次セッションが生きているか否かの状況確認を行い、

「死んでいる」セッションと確認できたセッションを削除していくので、削除ミスの可能性を極めて小さくすることができる。また、キープアライブパケットを使用しなくても「死んでいる」セッションを削除できるので、キープアライブパケットに対する課金がなくなり、移動端末400のユーザは通信コストを削減することができる。

【0039】 [2-2-2. 同一ユーザが再度セッション設定要求した場合] 次に、図8を参照しながら、移動端末411がセッション設定後にいったんパケットゲートウェイ360との接続を切断し、再接続後にセッション設定要求を行うことによって、同一ユーザが再度セッション設定要求した場合の動作について説明する。図8に示す例においては、移動端末411が最初にパケットゲートウェイ360に接続したときに割り当てられるIPアドレスは“123.456.78.9”であり、切断後に再接続したときに割り当てられるIPアドレスは“223.456.78.9”である。

【0040】 移動端末411のユーザインターフェイスからユーザIDおよびパスワードが入力されると(S201)、移動端末411は、ユーザID“Client1”としてセキュリティゲートウェイ110へのセッション設定要求を行う(S202)。このとき、セッション制御部115は、セッション情報記憶部116に記憶されているセッション情報を参照して同時接続セッション数の範囲内であると判定し、新たにセッション情報を生成する。この新たなセッション情報には、この時点で最も大きなセッション番号#1が付される。新たなセッション情報を生成するとセキュリティゲートウェイ110は、移動端末411に対してセッション設定の応答を行い(S203)、移動端末411と企業LAN100との仮想私設網210を介した通信を行うことができるようになる。

【0041】 その後移動端末411とパケットゲートウェイ360との接続が切断されると、セッション番号#1の付されたセッションは「死んだ」状態となるがセキュリティゲートウェイ110は移動端末412とパケットゲートウェイ360との接続が切断されている状態は検出しないので、セッション番号#1の付されたセッション情報はそのままセッション情報記憶部116に保存される。そして、移動端末411がパケットゲートウェイ360に再接続し、IPアドレス“223.456.78.9”が割り当てられる(S205)。ここで、移動端末411のユーザインターフェイスからユーザIDおよびパスワードが入力されると(S206)、移動端末411は、ユーザID“Client1”としてセキュリティゲートウェイ110へのセッション設定要求を行う(S207)。このとき、セッション制御部115は、セッション情報記憶部116に記憶されているセッション情報を参照して同時接続セッション制限数をオーバーしたことを検出

し、当該セッション情報に対応したIPアドレス“123.456.78.9”を宛先とした状況確認メッセージを送信する(S208)。

【0042】 移動端末411とパケットゲートウェイ360との接続が切断されたときに移動端末411に対するIPアドレス“123.456.78.9”の割り当ては解放されているので、IPアドレス“123.456.78.9”を宛先とした状況確認メッセージに対する応答は行われず(S209)。そこで、セッション制御部115は、状況確認を行ったセッション情報を削除し、ステップS207におけるセッション設定要求に対する新たなセッション情報(図中セッション番号#n)を生成する。新たなセッション情報を生成するとセキュリティゲートウェイ110は、移動端末411に対してセッション設定の応答を行い(S210)、移動端末411と企業LAN100との仮想私設網210を介した通信は、IPアドレス“123.456.78.9”から“223.456.78.9”に引き継がれて、継続して行うことが可能となる。

【0043】 このように、移動端末411がセッション設定後にいったんパケットゲートウェイ360との接続を切断し、再接続後にセッション設定要求を行うような場合には、セッション資源の枯渇を待たずに「死んでいる」セッションを早期に削除することができるので、セッション状態をより正確に管理することができるようになる。

【0044】 [2-2-3. 不正接続を防止する場合] 次に、図9を参照しながら、移動端末411がユーザID“Client1”としてセッション設定後、ハッカーが移動端末420からユーザID“Client1”としてセッション設定要求した場合の動作について説明する。図9に示す例においては、移動端末411がパケットゲートウェイ360に接続したときに割り当てられるIPアドレスは“123.456.78.9”であり、移動端末411がパケットゲートウェイ360に接続したときに割り当てられるIPアドレスは“987.654.32.1”である。

【0045】 移動端末411のユーザインターフェイスからユーザIDおよびパスワードが入力されると(S301)、移動端末411は、ユーザID“Client1”としてセキュリティゲートウェイ110へのセッション設定要求を行う(S302)。このとき、セッション制御部115は、セッション情報記憶部116に記憶されているセッション情報を参照して同時接続セッション数の範囲内であると判定し、新たにセッション情報を生成する。この新たなセッション情報には、この時点で最も大きなセッション番号#1が付される。新たなセッション情報を生成するとセキュリティゲートウェイ110は、移動端末411に対してセッション設定の応答を行い(S303)、移動端末411と企業LAN100との仮想私設網210を介した通信を行うことができるようになる。

【0046】次に、ハッカーが不正に入手したユーザID “Client1” およびパスワードを用いて、移動端末420からユーザID “Client1” としてセキュリティゲートウェイ110へのセッション設定要求を行う（S304）。このとき、セッション制御部115は、セッション情報記憶部116に記憶されているセッション情報を参照して同時接続セッション制限数をオーバーしたことを検出し、当該セッション情報に対応したIPアドレス “123.456.78.9” を宛先とした状況確認メッセージを送信する（S305）。このメッセージはIPアドレス “123.456.78.9” が割り当てられたままになっている移動端末411に到達するので、移動端末411は、状況確認メッセージに対する正常な応答を行う（S306）とともに、ユーザインターフェイスに警告メッセージを表示させる（S307）。応答を受けたセキュリティゲートウェイ110は、ステップS304でうけたセッション設定要求を拒絶して（S308）、拒絶したセッション設定要求が示すユーザID “Client1” とIPアドレス987.654.32.1” とを対応つけてアクセス拒否情報として登録する。

【0047】その後、移動端末420から再度セッション設定要求があった場合には（S309）、セキュリティゲートウェイ110はアクセス拒否情報を参照することによって、ユーザID “Client1” を示すセッション設定要求であっても、IPアドレス987.654.32.1” であればハッカーからの要求であると判定してセッション設定を拒絶することができる（S310）。また、移動端末411のユーザは、ユーザインターフェイスに表示される警告メッセージなどによりハッカーの存在を認識し、パスワードの変更などの対処を行う。

【0048】このように、悪意の第三者（ハッカー）が正当なユーザの認証情報を不正に入手してセッション設定要求を行う場合には、すでに記憶されているセッション情報の中から同一の認証情報を有するIPアドレスに対して状況確認メッセージを送信することによって、ハッカーによる不正な接続を防止できるようになる。

【0049】[3. 変形例] 本発明は、上述した実施形態に限定されるものではなく、以下のような各種の変形が可能である。

【0050】上記実施形態においては、クライアント側の端末装置を移動端末400を例として説明したが、インターネット接続点と通信網を介して接続可能であればどのようなものでもよい。同様に、上記実施形態では、サーバ側のネットワークを企業LAN100を例として説明したが、インターネットとの接続が可能であればどのようなものでもよく、行政サービス用のネットワークや家庭内のインターネット対応機器で構成したネットワークなどでもかまわない。また、通信網もPDCパケット通信網300に限らず、送受信データ量に対して課金されるものであれば他の通信網であってもよい。インタ

ーネット接続点についても、パケットゲートウェイ360に限らず他のプロバイダであってもよいのはもちろんである。

【0051】上記実施形態では、セッション設定要求に含まれる認証情報として、ユーザIDおよびパスワードを例として説明したが、これに限らず、デジタル署名など他の情報であってもよい。また、アドレス情報についても、IPアドレスに限らず、クライアントの端末と特定する他の情報であってもよい。

【0052】上記実施形態では、削除候補セッション情報を選択するための所定の規則としては、FIFOあるいはLRUすなわち、選択される優先順位は生成されてからの経過時間が長いあるいは最後に使用されてからの経過時間が長いセッション情報である程高いものを例として説明しているが、これに限らず、セッションが「死んでいる」可能性が高いものを選択できれば他の規則であってもかまわない。また、生成されてからの経過時間が長いあるいは最後に使用されてからの経過時間を示す情報として、上記実施形態ではセッション番号を用いて説明しているが、これに限らず、時刻そのものをセッション情報に含ませるようにしてもよいし、他のパラメータを用いてもかまわない。

【0053】

【発明の効果】以上説明したように、本発明によれば、クライアントとサーバとを接続する仮想私設網において、安定的な通信を確保しながら低コストでセッション情報の資源枯渇を防止するが可能となる。

【図面の簡単な説明】

【図1】 実施形態の全体構成を示す図である。

【図2】 セキュリティゲートウェイの構成を示す図である。

【図3】 記憶する各種情報を説明する図である。

【図4】 セキュリティゲートウェイの動作を説明するフローチャートである。

【図5】 セッション設定処理を説明するフローチャートである。

【図6】 不正アクセス防止処理を説明するフローチャートである。

【図7】 総セッション数制限をこえた場合の具体的な動作を説明するシーケンスである。

【図8】 同一ユーザが再度セッション設定要求した場合の具体的な動作を説明するシーケンスである。

【図9】 不正接続を防止する場合の具体的な動作を説明するシーケンスである。

【符号の説明】

100…企業LAN、

110…セキュリティゲートウェイ、

200…インターネット、

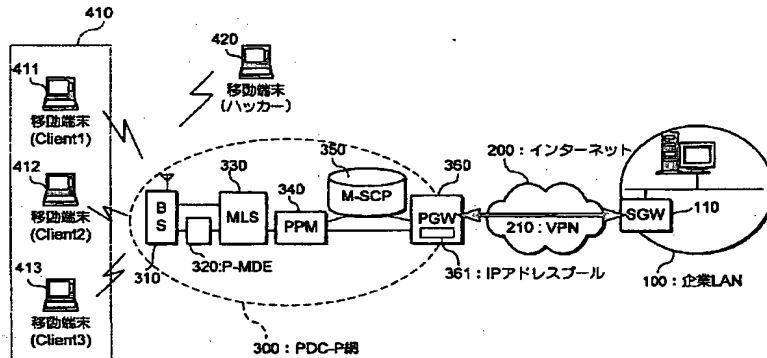
210…仮想私設網

300…移動通信網、

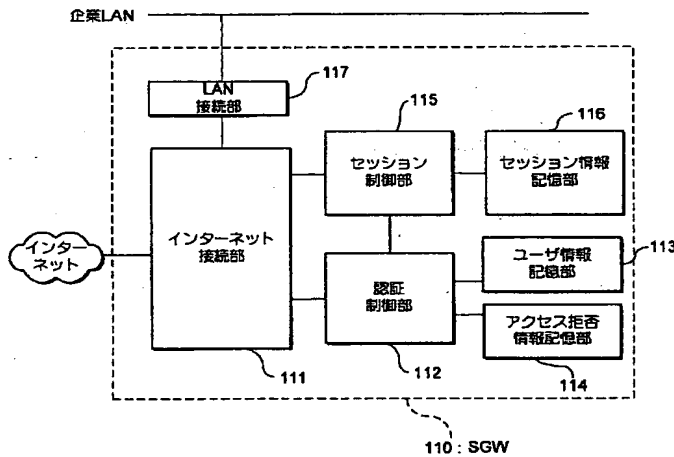
310…基地局、  
 320…パケット用基地局変復調装置、  
 330…加入者交換機、  
 340…パケット加入者系処理装置、

350…移动通信サービス制御装置、  
 360…パケットゲートウェイ、  
 361…IPアドレスプール、  
 411、412、413、420…移動端末。

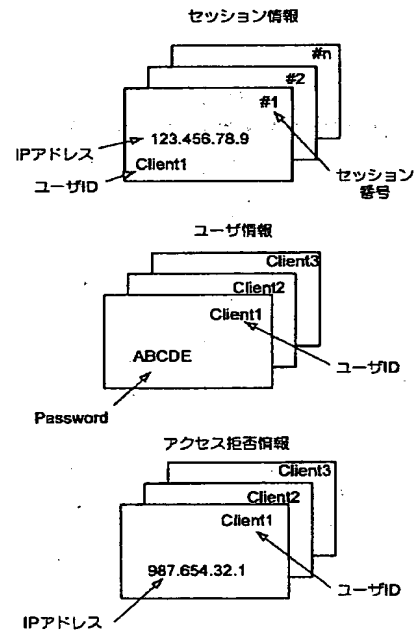
【図1】



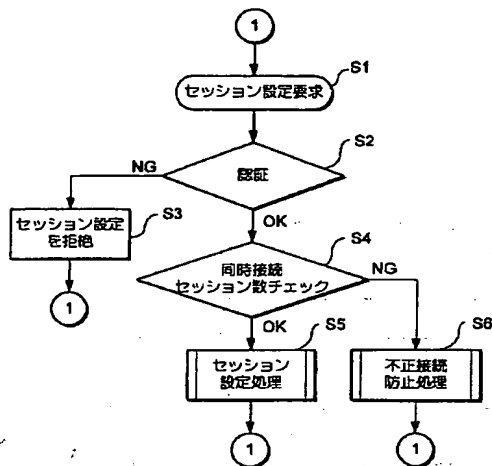
【図2】



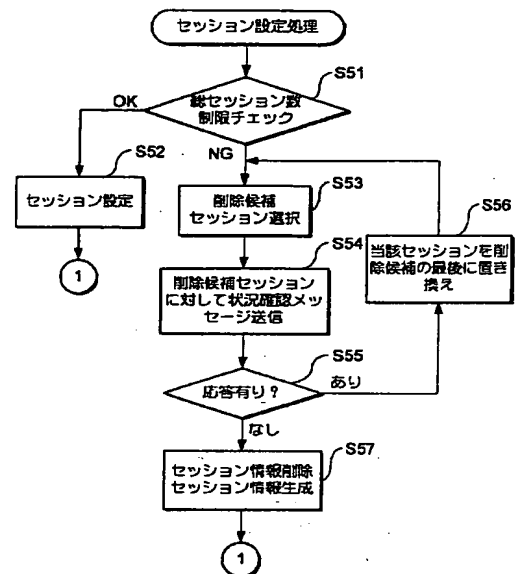
【図3】



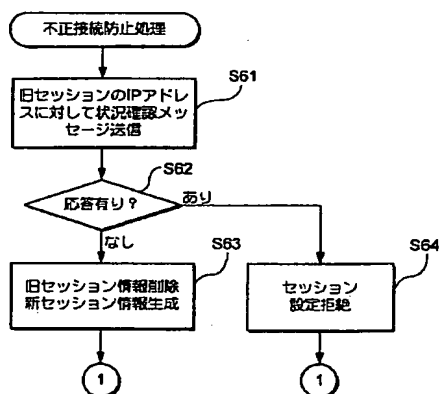
【図4】



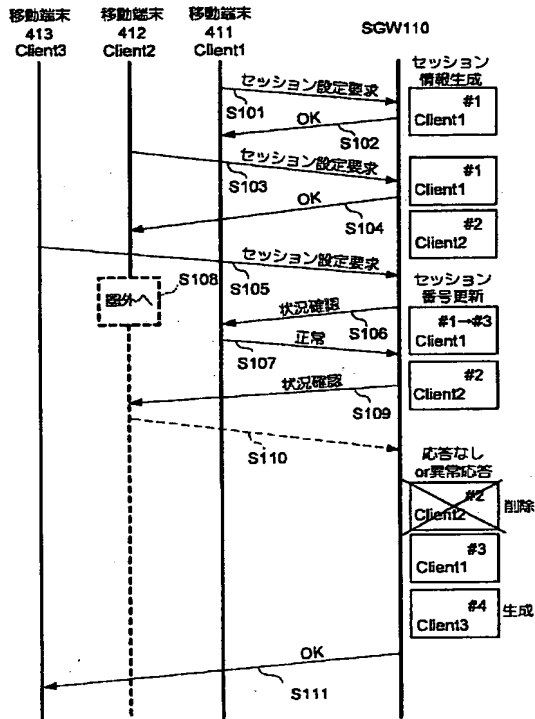
【図5】



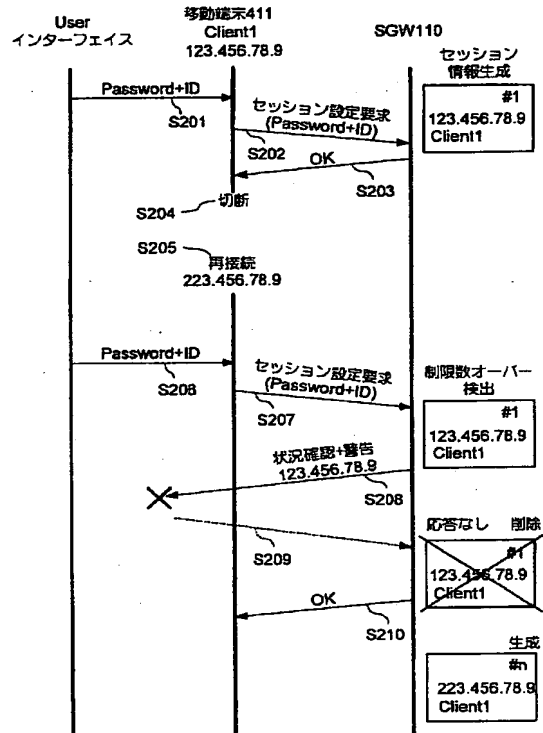
【図6】



【図7】



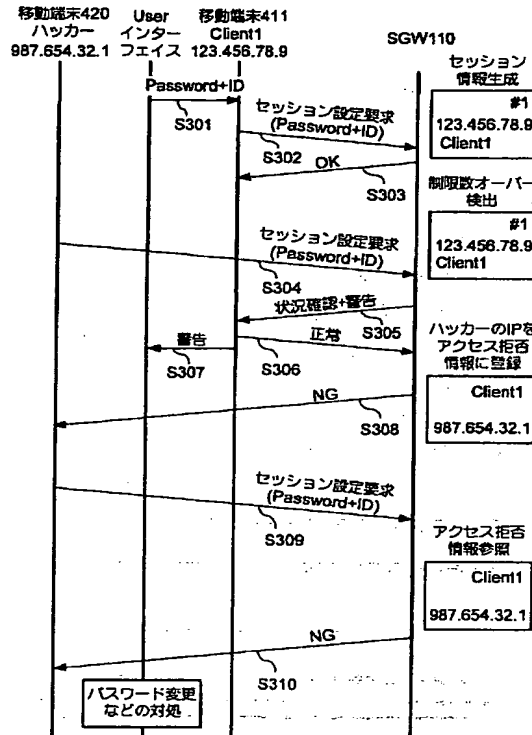
【図8】



BEST AVAILABLE COPY



【図9】



フロントページの続き

(72)発明者 関口 克己  
東京都港区虎ノ門二丁目10番1号 エヌ・  
ティ・ティ移動通信網株式会社内

Fターム(参考) 5B089 GA31 HA01 KA12 KA16 KB06  
KB11 KC28 KC39 KC51 KC54  
KC58 KG01 KG03 MA02 MC01  
5K030 GA15 HA08 KA04 KA05 LA03  
LB02 LC18 LD20

THIS PAGE BLANK (USPTO)

1965-1966